Building Automation System (BAS)

(formerly know as EMCS)

Network Connectivity

(16 April 2008)

Will White (Huntsville), Dr. Steve Briggs (FDE)

US Army
Corps
of Engineers

Outline:

- Describe BAS
  - As “we” (control/HVAC engineers) understand it
  - As it appears to an IT/IA person
- Case studies
- Difficulties encountered
  - We don’t fit the process mold
  - We aren’t IT/IA people
  - Regs/DOIM seem in flux

US Army
Corps
of Engineers

What BAS is NOT

- NOT a centrally funded program
- NOT mandated/required in any manner
- NOT provided by a single vendor
  - Even a single installation is intended to be multi-vendor
- NOT a specific set of hardware/software
- NOT static – we are constantly adding/growing
- NOT a system that easily fits the DIACAP mold

US Army
Corps
of Engineers

As a concrete example:
CorpsLon is:
The system defined by:

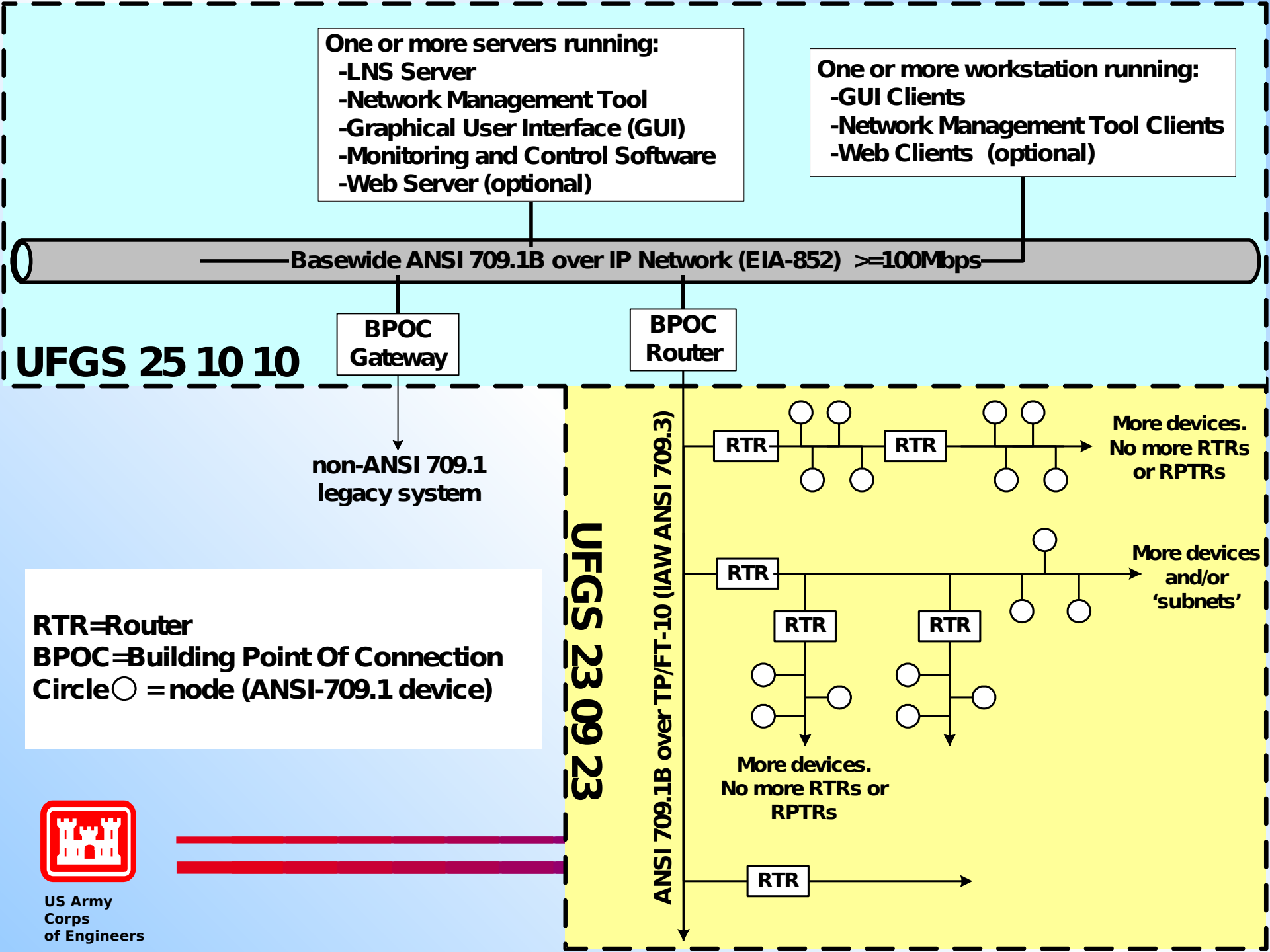
- Hardware/Software in the building:
  - UFGS 23 09 23: Direct Digital Control for HVAC and Other Local Building Systems
  - To include any additional DIACAP requirements
- Hardware/Software at the installation-wide front-end
  - UFGS 25 10 10: Utility Monitoring and Control System (UMCS)
  - To include any additional DIACAP requirements
- UFC 3-410-02 (building) and UFC 3-401-01 (front-end)

US Army
Corps
of Engineers

Other example BAS architectures:

- Johnson Controls Metasys
- Tridium Niagara Framework
- BACnet systems

- We will focus on the “CorpLon” architecture
- Will highlight significant differences


One or more servers running:
-LNS Server
-Network Management Tool
-Graphical User Interface (GUI)
-Monitoring and Control Software
-Web Server (optional)
One or more workstation running:
-GUI Clients
-Network Management Tool Clients
-Web Clients (optional)
Basewide ANSI 709.1B over IP Network (EIA-852) >=100Mbps
BPOC Gateway
BPOC Router
UFGS 25 10 10
non-ANSI 709.1 legacy system
UFGS 23 09 23
ANSI 709.1B over TP/FT-10 (IAW ANSI 709.3)
RTR
RTR
More devices. No more RTRs or RPTRs
RTR
More devices and/or 'subnets'
RTR
RTR
More devices. No more RTRs or RPTRs
RTR
RTR=Router
BPOC=Building Point Of Connection
Circle ○ = node (ANSI-709.1 device)
US Army Corps of Engineers

What BAS is:

- Buildings with local controls (not important in this context)
- A network connecting everything together
- One or more servers:
  - Standard WinXX PCs
  - Running Vendor-specific software providing:
    - Ability for O&M staff to monitor and control
    - Schedule things ON/OFF
    - Monitor health of mechanical equipment (alarms)
    - Log data for troubleshooting
    - Take temporary corrective action (override)
    - Execute global optimization strategies (demand limit)
- Multiple clients providing GUIs to the servers

US Army
Corps
of Engineers

Functionality / Mission Impact / Exploitability

- Controls Heating, Ventilation, and Air Conditioning (HVAC) equipment
- Can control this equipment, turn on/off, etc.
- Can’t do anything from control system that you can’t do manually from the equipment
- Controls generally co-located with equipment
- Not intended to support mission critical equipment
  - Put a “disclaimer” in spec
  - Not for Command & Control
  - Not for data centers
  - For barracks, admin, dining halls, schools, etc.

US Army
Corps
of Engineers

Why A Post Needs a BAS

- Allow energy manager to meet efficiency goals
- Comply with EPAct 2005 and Executive orders
- Conserve energy resource
- Reduce pollution
- Provide timely response to system failures
- Save dollars and labor
- Maintain occupant comfort

US Army
Corps
of Engineers

IT view of BAS:
Buildings:

- Lots of buildings with lots of “Stuff”
  - Controllers, sensors, actuators, networking
- Building controls are microprocessor-based but not capable of executing “arbitrary” programs
  - More at the level of embedded controllers, typically very slow by today’s IT standards
  - Capabilities limited by firmware in the device
- Building has a control network, but it’s not IP
  - Typical 78 kbps vs 100 Mbps
  - Not IP, no IP/TCP/UDP/ICMP, etc. stack
  - Protocols more suited for building automation

US Army
Corps
of Engineers

IT view of BAS:
Front End Server/Client:

- Server:
  - Front end for monitoring and control of building systems
  - WinXX PC, probably with a server OS
  - Probably with a web server
  - Probably with a database server
  - Loaded with vendor specific software
- Clients typically access front end via web interface
  - Standard WinXX PCs
  - May have vendor specific software, or just a browser
  - Any machine on LAN can be a client
  - In reality, can limit to a few machines
  - Isolate network connection via VLAN or VPN

US Army
Corps
of Engineers

IT view of BAS:
Network:

- Control data over an IP network
- Buildings “only” talk to the server
- Prefer to use the existing post-wide DOIM LAN
  - Responsibility for maintenance of IP with DOIM
  - Responsibility for securing LAN with DOIM
- LonTalk is tunneled over UDP port 1628 and 1629
- BACnet also uses a tunneling method of BACnet over IP
- In other cases, control data is sent via HTTP
  - Johnson Metasys
  - Tridium
  - IP-based controllers are still the exception
- Clients “always” talk to server via HTTP
- Network can be completely isolated from everything else
  - Typically via DOIM-implemented VLAN and/or VPN

US Army
Corps
of Engineers

IT view of BAS:
System Growth:

- Add building
  - Buildings have lots of non-IP devices
  - No IA impact
  - Adding devices doesn’t have an IA impact
- Add device that converts control protocol to IP
  - One (few) per building
  - May be tunneling device
  - May be HTTP device
  - Only a small number of types of these devices
- Add IP drop – minimal IA impact; DOIM responsibility
- Configure server – no IA impact

US Army
Corps
of Engineers

Case Study: Army Post I

- BAS is “hoping” to fall under DOIM ATO
- Problems with getting Networthiness
  - Networthiness paperwork incorrect
  - Required re-submittal
- Automatically pushed security updates have broken UMCS (front end clients)
- Need to avoid pushing updates in some cases
- Have good coordination with DOIM
  - DOIM is not halting work awaiting approval

US Army
Corps
of Engineers

Case Study: Army Post C

- DOIM does not require separate DIACAP
- BAS is covered under DOIM's ATO for post-wide LAN
- Working on CON, but not in system yet….
  - DOIM wants BAS to have this, but has not halted connection of system because of lack of CON
- Seems to be good relationship between BAS owners and DOIM
- DOIM is requiring dedicated machines for all BAS client machines to ease security concerns

US Army
Corps
of Engineers

Case study: Army Post T

- DOIM is requiring DIACAP and Networthiness
- Contractor originally told they would not need DIACAP
- Later, DOIM required DIACAP and did not allow connection to network
- Major disruption of contractor
- Post-wide LAN is not as secure as it “should” be
- Currently, in DIACAP/Networthiness “Catch-22”
  - Can’t install software without Networthiness
  - Can’t get Networthiness without ATO
  - Can’t get ATO without a system to test
  - Can’t test system without software installed
- Awaiting DOIM to put system in APMS so we can proceed with getting CON

US Army
Corps
of Engineers

Case Study: Interactions with IASED

- Mutual education about our system and IA requirements
- Initial focus on building network (non-IP) vulnerabilities
  - Building control network is readily accessible
    - Thermostats
    - In suspended ceilings
  - Initially a security concern
  - After discussion with security engineer, not a concern
    - Inherent limitations of control network speed and protocol
    - Inherent “filters” at IP platform interconnect device
      - Lon to IP “router” only passes control protocol
- Major outcome: building network (non-IP) not of concern

US Army
Corps
of Engineers

Lessons learned:

- Every installation seems to have slightly different requirements
- Inconsistencies between DOIMs
- Network security needs addressing
  - At Fort T, BAS is held up because of this
  - Poor IP security impacts our system
- Focus needs to be on front-end server, not building controls
- BAS hardware, software, network, and protocols not understood by IA/IT people
  - Have worked with IASED
  - Need to work with other ACAs?
- DIACAP requirements not clearly understood by the HVAC community: project engineers, installers, and maintainers
- Need to determine costs and get this in future budgets
  - What are the costs: up front and ongoing?
  - Does every installation need to pay this separately?

US Army
Corps
of Engineers

Thinking “outside the box”

- Does the BAS need its own DIACAP?
  - Or be covered under DOIM post-wide ATO?
  - Can there be a “type” accreditation?
- BAS software broken by pushed security upgrades
  - Is there a better way to manage these machines?
- We typically contract out maintenance
  - How can we handle contractor access to the LAN?
- What is the connection between Networthiness and DIACAP?
- We struggle with inconsistent DOIMs
  - How can we get consistent direction from them?

US Army
Corps
of Engineers

Smart Grid
“off the cuff remarks”

- Use of local generation and distribution assets in a Distributed manner
  - Hospital diesel generators may be used for supplemental power elsewhere on post
- Allows for distributed control of generation assets and load shedding
- Control is very dependent on IP network
- Different risk environment than BAS
  - Significant risk of mission impact if network compromised as local assets may be rendered unavailable by network controls
- May be very difficult to meet IA controls

US Army
Corps
of Engineers

Contact Information

- Will White
  - Will.white@uasce.army.mil
  - 256-895-1739
- Dave Schwenk
  - David.m.schwenk@erdc.usace.army.mil
  - 217-373-7241
- Joe Bush
  - Joseph.Bush3@us.army.mil
  - 217-898-5408
- Dr. Steve Briggs
  - steveb@facilitydynamics.com
  - 217-356-3218

US Army
Corps
of Engineers